ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

Comparative analysis of optical transformation for image encryption

Zhonglin Yang[1,*], Yanhua Cao[1], Xiangyu Liu[1], Zhengjun Liu[2], Hang Chen[1,3]

[1]School of Space Information, Space Engineering University, Beijing, 101416, China
[2]Department of Automation Measurement and Control, Harbin Institute of Technology, Harbin, 150001, China
[3]Université de Lorraine, CNRS, CRAN UMR 7039, Nancy, 54000, France
**Corresponding author: hitchenhang@foxmail.com*

Abstract: *This paper first introduces the characteristics of optical transformation, and then according to the relationship between optical transformation and cryptography, it is suitable for image encryption, followed by a detailed description of various common optical transformation, and comparative analysis.*

Keywords: *optical transformation, Fresnel, Fractional Fourier, Gyrator, Linear regular*

1. Introduction

The application of image has penetrated into every aspect of people's life[1-2]. The development of the Internet[3-4] has greatly promoted the progress of image technology, but also brought high security risks. Criminals can intercept the transmitted images for use or tamper with them. This requires the image to be encrypted before transmission. However, the increasing amount of image data[5-6] puts forward higher requirements and tests for encryption technology.

Refregier and Javidi first proposed the optical image encryption algorithm double random phase coding technology in 1995 [7]. Since then, the classical double-random phase coding technology has been extended from Fourier transform domain to fractional Fourier transform domain and Fresnel transform domain, and the optical dimension of hidden secret information has also been extended from the initial phase information to amplitude information or polarization information. In recent years, many foreign scholars have applied different optical processing techniques to optical encryption algorithms and verified the feasibility of these methods through experiments. Prof. Javidi's group at the University of Connecticut, Prof. Sheridan's group at the University of Dublin, Prof. Zhang's group at the University of Birmingham, Prof. Quan's group at the National University of Singapore, and Prof. Alfalou's group at ISEN in France have done a lot of meaningful work on the design of optical image encryption algorithms.

Image encryption algorithm based on optical transform is no longer limited to classical double random phase coding algorithm, but expanded to different transform domains, such as Fourier transform[8-9], fractional Fourier transform[10-11], Fresnel transform[12-13], Gyrator transform[14-15], linear regular transform[16] and so on. In this paper, several commonly used optical transformation are compared and analyzed, and the optimal selection of optical transformation is obtained under general circumstances.

The rest of this paper is organized as follows. Section 2 introduces the cryptographic advantage of optical transformation and its relation to cryptography in detail. Section 3 gives a detailed introduction and comparative analysis of common optical transformation. Finally, the concluding remarks are summarized in the last section.

2. Basic knowledge of optical transformation

2.1 The advantage of optical transformation

Optical image encryption technology has the advantages of parallel processing, large key space, strong robustness, fast computing speed and high design freedom. The most prominent advantages are parallel processing, large key space and fast computing speed.

ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

Parallel processing: Parallel data processing is an inherent ability of optical systems, in which any pixel in an image can be simultaneously transmitted and processed. The more complex the image is and the more information is, the more obvious this advantage will be.

Large key space: the wavelength, amplitude, phase, intensity, and spatial frequency of the light can be used as the key of the system.

Fast calculation speed: through a light irradiation can be completed a encryption, fast implementation.

2.2 The relationship between chaos theory and cryptography

Table 1: The relationship between optical transformation and cryptography

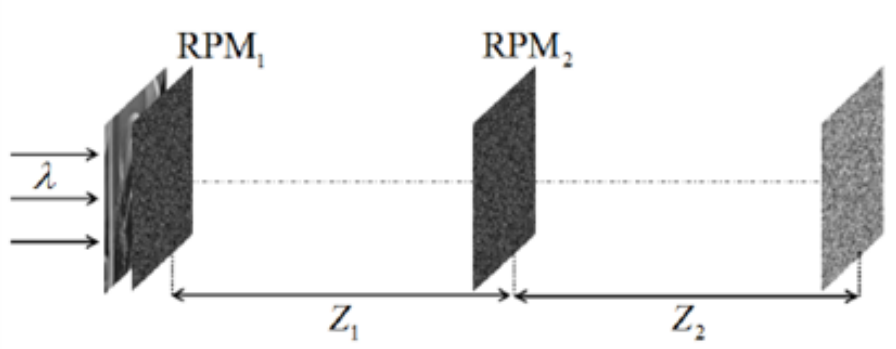
name	cryptography	optical transformation
Similarity	Encryption round number	The number of iterations
	Controlled by and sensitive to a key	Controlled by parameters and initial conditions and is extremely sensitive to them
	Chang statistical characteristics through obfuscation and substitution	Change statistical properties by scrambling and diffusion
Difference	Mapping on a finite set of integers	Mapping on the set of complex
	There are more complete evaluation and performance indicators	There are no comprehensive evaluation and performance indicators

Optical transformation and cryptography have the following similarities and differences, as shown in Table 1.

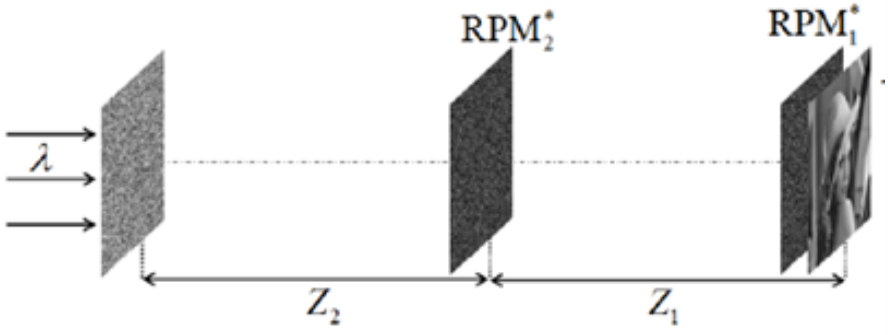
Because there are many similarities with the password system, so the optical transformation to image encryption has a great advantage, and the difference between the password system, is in the application process need to pay attention to the place.

3. Introduction and comparison of commonly used optical transformation

3.1 Fresnel diffraction



(a) The encryption process



(b) The decryption process

Figure 1: Optical implementation device of DRPE encryption method based on Fresnel transform

ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

DRPE encryption in the Fresnel transform domain relies on a random phase plate rather than a Fourier transform lens. The optical encryption and decryption process of Fresnel transform is shown in Fig.1. In a cryptographic system, RPM_1 and RPM_2 are two random phase plates placed at different distances. The plane optical wavelength λ and distance z of Fresnel transform can be used as additional key.

The expression is as follows

$$f(x,y)=\frac{\exp(j2\pi/\lambda)}{j\lambda z}\iint f_0(x_0,y_0)\times\exp\left[j\pi\left[(x_0-x)^2+(y_0-y)^2\right]/(\lambda z)\right]dx_0dy_0 \quad (1)$$

3.2 Fractional Fourier transform

The cryptographic expression for the fractional Fourier transform can be written as follows

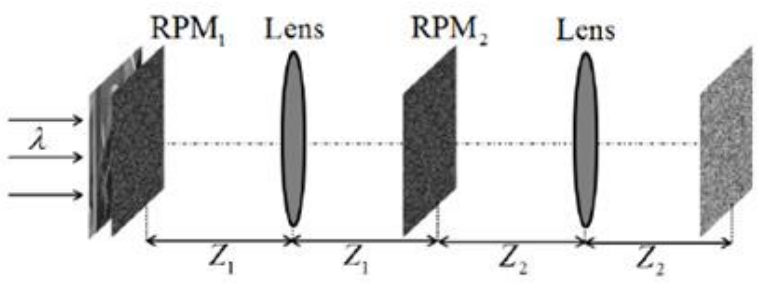
$$f(x,y)=A_\varphi\iint f_0(x_0,y_0)\exp\left\{j\pi\left(\frac{x_0^2+x^2}{\tan\varphi}-\frac{2(x_0x+y_0y)}{\sin\varphi}+\frac{y_0^2+y^2}{\tan\varphi}\right)\right\}dx_0dy_0 \quad (2)$$

Where, $f_0(x_0,y_0)$ and $f(x,y)$ are the input image and the transformed image respectively, $\varphi=\frac{a\pi}{2}$ and a are the transformation order; The phase factor A_φ is defined as follows:

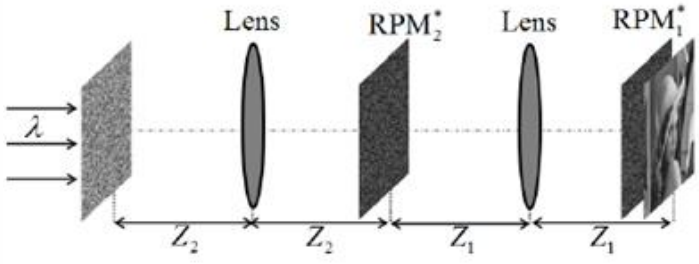
$$A_\varphi=\frac{\exp\left[-j\pi\,\mathrm{sgn}(\sin\varphi)/4+j\varphi/2\right]}{|\sin\varphi|^{1/2}} \quad (3)$$

Where, $\mathrm{sgn}(.)$ is a symbolic function.

The optical device of fractional Fourier transform is shown in Fig.2.



(a) The encryption process



(b) The decryption proces

Figure 2: Optical implementation device of DRPE encryption method based on fractional Fourier transform

ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

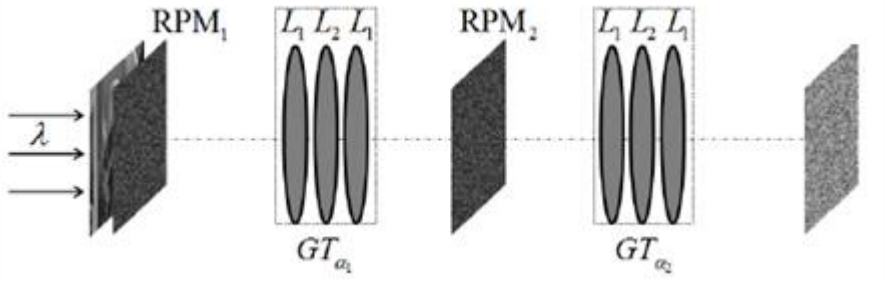
3.3 Gyrator transform

Gyrator transformation is realized by a combination of three generalized lenses and its mathematical expression is shown below:

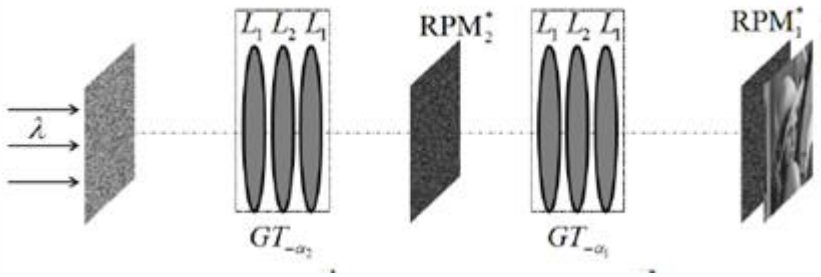
$$f(x,y)=\frac{1}{|\sin\alpha|}\iint f_0(x_0,y_0)\exp\left\{j2\pi\frac{(xy+x_0y_0)\cos\alpha-(x_0y+xy_0)}{\sin\alpha}\right\}dx_0dy_0 \quad (4)$$

Where, $f_0(x_0,y_0)$ and $f(x,y)$ are the input image and the transformed image respectively, and α is the order of Gyrator transformation, which can be used as an extra key.

The optical implementation device of DRPE encryption method based on Gyrator transformation is shown in Fig.3. In the encryption process, two sets of lenses need to be placed behind *RPM1* and *RPM2* respectively. The decryption process is the opposite.



(a) The encryption process



(b) The decryption process

Figure 3: Optical implementation device of DRPE encryption method based on Gyrator transform

3.4 Linear canonical transformation

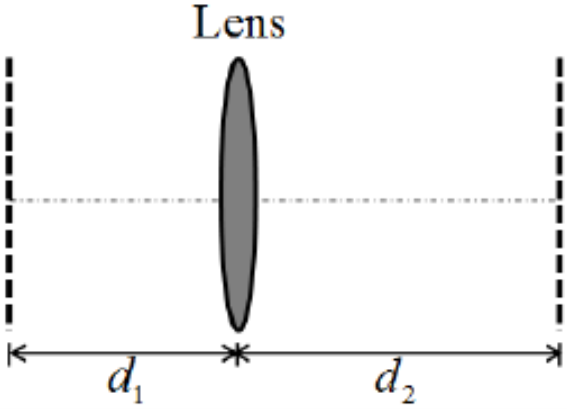


Figure 4: The diagram of Arnold transformation

Fig.4 shows the optical implementation device of linear regular transformation. Figure 2-12 shows the optical encryption and decryption process of DRPE method based on linear regular transformation. The two-dimensional linear regular transformation of the image is defined as follows:

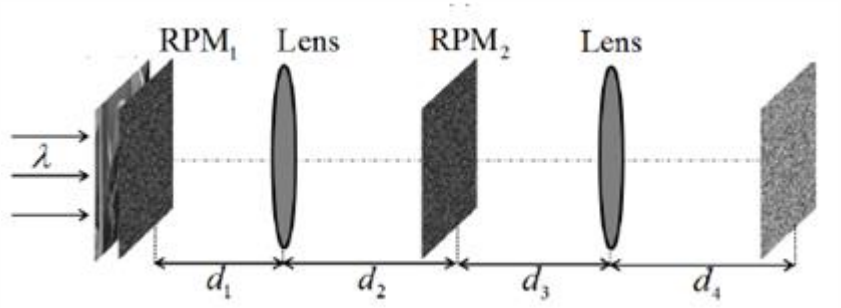
ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

$$f(x,y)=\sqrt{\beta}\bullet\exp\left\{\frac{-j\pi}{4}\right\}\iint f(x,y)\\ \bullet\exp\left\{\alpha\left(x_0^2+y_0^2\right)-2\beta(x_0x+y_0y)+\gamma(x^2+y^2)\right\}dx_0dy_0 \tag{5}$$

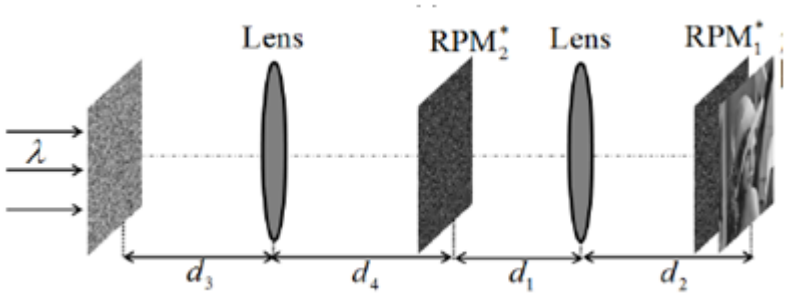
Where, $f_0(x_0,y_0)$ and $f(x,y)$ respectively represent the input image and the transformed image; α, β and γ are the parameters of transformation; And focal length f, distance d_1 and d_2 satisfy:

$$\begin{cases}\alpha=\dfrac{d_1-f}{\lambda\left[f\left(d_1+d_2\right)-d_1d_2\right]}\\ \beta=\dfrac{f}{\lambda\left[f\left(d_1+d_2\right)-d_1d_2\right]}\\ \gamma=\dfrac{d_2-f}{\lambda\left[f\left(d_1+d_2\right)-d_1d_2\right]}\end{cases}$$

Where, λ is the wavelength of plane light.



(a) The encryption process



(b) The decryption process

Figure 5: Optical implementation device of DRPE encryption method based on linear regular transformation

3.5 Classification analysis and comparison

There are five types of optical transformation. Five encryption systems are tested, as shown in Table 2. All of these five optical encryption systems can fully decrypt the original image from their own encrypted image. Comparing the encryption performance of each optical system, fractional Fourier transform encryption system, Gyrator transform encryption system and linear regular transform encryption system perform better in the correlation between adjacent pixels. In terms of anti-noise attack, fractional Fourier transform, Gyrator transform and linear regular transform encryption system perform better than Fourier transform plus Fresnel transform encryption system. Fractional Fourier transform, Gyrator transform and linear regular transform have better performance in the correlation between adjacent pixels and anti-shear attack. In the realization of optical devices, Gyrator transform and Fresnel transform are simpler. In practical applications, not only various encryption properties should be

ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

considered, but also the realization of optical devices should be considered. Therefore, Gyrator transform and Fresnel transform are selected for further study in this paper.

Table 2: Performance comparison

Performance / Name	The correlation between adjacent pixels	Anti-noise attack	anti-shearing attack	Realization of optical devices
Fourier transform	×	×	×	×
fractional Fourier transform	√	√	√	×
Fresnel transformation	×	×	×	√
Gyrator transformation	√	√	√	√
Linear canonical transform	√	√	√	×

In addition to the advantages of parallel processing capability and multiple degrees of freedom, optical system also has the following two limitations:

First, the ability to resist selective plaintext attack needs to be improved. In a large number of existing optical image encryption algorithms, the key stream used for diffusion is related only to the key. This means that if the key is not changed, the same key stream will be used to encrypt different plaintext images, making it vulnerable to select plaintext attacks. For example, an attacker can construct a plaintext image (such as an all-white or all-black image) composed of special pixel values and apply an encryption system to encrypt the image. One of the basic requirements of modern cryptography is that the cryptographic algorithm itself is completely open. Based on the mastery of the encryption algorithm, the attacker can get the used key stream by comparing the ciphertext image with the plaintext image.

Second, the optical encryption technology matching hyperspectral images is not perfect. If the optical encryption scheme used for color image is directly used for hyperspectral image encryption, it will result in low security or low efficiency. Usually there are two kinds of cooking. One is to encrypt different channels separately for hyperspectral image encryption. If the encryption scheme is the same, a large number of ciphertext with the same key will be generated. If the encryption schemes are different, the encryption efficiency decreases. In the other scheme, different channels are combined into a single channel, which is used for hyperspectral image encryption, with complex preprocessing and low efficiency.

Table.3: The relationship between chaos theory and cryptography

name	dimension	classification
chaos	One	Logistic mapping, Chebyshev mapping, Tent mapping
	Two	Henon mapping, Duffing mapping, Tinkerbell mapping, Lozi mapping, Arnold transformation
	Three	3D Arnold transform, hyperchaos

4. Conclusion

In practical application, the beam can be encrypted once through a lens, which is fast and efficient, but in computer simulation of optical encryption needs to write a strict program to verify. Efficient and secure encryption scheme is the key to guide physical practice. How to design optical encryption scheme for optical transform with excellent performance and verify its security performance is the focus of practical research.

References

[1] Mendoza F, Aguilera J M. Application of Image Analysis for Classification of Ripening Bananas [J]. Journal of Food Science, 2004.
[2] Button M R, Staffurth J N. Clinical application of image-guided radiotherapy in bladder and prostate cancer. [J]. Clinical Oncology, 2010, 22(8):698-706.
[3] Greiner G. MIL-STD-188-220B-based digital tactical radio networks: the development of the Internet has significantly changed the quality and quantity of communications. If these technical standards can be incorporated in military communications, conventional tactica [J]. Probus, 2004, 120(2):172-173.
[4] Cho H, Kwon M, Choi J H, et al. Development of the Internet addiction scale based on the Internet

ISSN 2616-5775 Vol. 5, Issue 5: 10-16, DOI: 10.25236/AJCIS.2022.050502

Gaming Disorder criteria suggested in DSM-5[J]. Addictive Behaviors, 2014, 39(9):1361-1366.
[5] V Stodden. Central to Scientific Research 1. enormous, and increasing, amounts of data collection:. 2014.
[6] Achong J M, Zhou H, Clarke I. Method and apparatus for increasing contrast in a digital image[J]. 2007.
[7] Refregier P, Javidi B. Optical image encryption using input plane and Fourier plane random encoding[C]// Optical Implementation of Information Processing. International Society for Optics and Photonics, 1995.
[8] Bracewell R. The Fourier transform and its applications [C]. American Association of Physics Teachers. American Association of Physics Teachers, 2002.
[9] Harris F J. USE OF WINDOWS FOR HARMONIC-ANALYSIS WITH DISCRETE FOURIER-TRANSFORM [J]. Proceedings of the IEEE, 1978, 66(1):51-83.
[10] Almeida, L. B. The fractional Fourier transform and time-frequency representations [J]. Signal Processing, IEEE Transactions on, 1994.
[11] Ozaktas H M, Arikan O, Kutay M A, et al. Digital computation of the fractional Fourier transform [J]. IEEE Trans Signal Process, 1996, 44(9):2141-2150.
[12] Ferraro P, Nicola S D, Coppola G, et al. Controlling image size as a function of distance and wavelength in Fresnel-transform reconstruction of digital holograms [J]. Optics Letters, 2004, 29(8):854-856.
[13] James D, Agarwal G S. The generalized Fresnel transform and its application to optics [J]. Optics Communications, 1996, 126(4-6):207-212.
[14] Rodrigo, Jos\u00e9, A, et al. Gyrator transform: properties and applications [J]. Opt Express, 2007.
[15] A Jos é, Rodrigo, Tatiana, et al. Gyrator transform: properties and applications. [J]. Optics express, 2007.
[16] Zamani P, Soltanianzadeh H. Compressive sensing cardiac cine MRI using invertible non-linear transform[C]. Electrical Engineering. IEEE, 2015.